Data Protection in the European Union: Current Status and Future Implications

BRIANA N. GODBEY*

ABSTRACT

Data protection and retention legislation are increasingly important in a society where an individual can communicate, buy and sale goods electronically, and post information on the internet, all on a global level. A side-effect of this increased access to the global community is the increased difficulty of regulating access to private information. However, some countries are responding by increasing their legislation over the transfer of information across their borders, and the European Union ("EU") is leading this charge. The EU implemented its original privacy directive in 1997 and since that time, every EU Member State has enacted some form of privacy legislation. EU Member States require that any state or entity seeking access to the information of their citizens must have comparable data protection standards in place. Therefore, in an effort to increase trade opportunities, several non-EU states have enacted such legislation as well. These privacy standards are the focus of this article, looking first at the basic aspects of the three main data protection sources: the European Union privacy directives, the European Council on Cybercrime and the Organisation for Economic Co-operation and Development, and the European Council on Cybercrime. This article also addresses specific legislation enacting data protection measures in the United Kingdom and the United States, and finally, it addresses some of the concerns associated with increased data protection.

I. INTRODUCTION

Data protection has been viewed as a fundamental human right in Europe since a decision by the German Federal Constitutional Court in 1983 recognized that there is a "right to informational self-determination."[1] Members of the European Community have been implementing their own privacy laws since 1970, with the vast

---

* The author is juris doctor candidate at The Ohio State University, Moritz College of Law, class of 2007. The author holds degrees from the University of North Texas, Bachelor of Arts, Political Science; Master of Arts, Political Science.

[1] CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS 16 (Oxford Univ. Press) (2003), citing Bundesverfassungsgericht [BverfGE] [Federal Constitutional Court], Nov. 15, 1983, 65 Entscheidungen des Bundesverwaltungsgerichts [BVerfGE] 1 (F.R.G.).

majority enacting some sort of national legislation by 1990.[2] These national legislative acts usually had four common factors:

> typically they apply to both public and private sectors; they apply to a wide range of activities, including data collection, storage, use and dissemination; they impose affirmative obligations (often including registration with national authorities of anyone wishing to engage in any of these activities); and they have few, if any, sectoral limitations.[3]

However, with establishment of the European Union ("EU"), the legislative acts regarding electronic privacy transfer were solidified first in the EU Directive from 1997 and finally, in its amended form in 2002.[4]

This article provides the reader with a foundation of knowledge of the important sources of data protection legislation internationally, including citations to the leading authorities on these institutions; and includes discussions on the major recent developments in the area of data protection and retention in the EU. The EU Directive, as the leading force of privacy regulation in the world, is the focus of the first section of this paper. Subsequent sections briefly discuss the other agencies regulating the transfer of electronic data, namely, the European Council on Cybercrime and the Organisation for Economic Co-operation and Development ("OECD") Guidelines, followed by a discussion of legislation from the United Kingdom and the United States in response to these regulations.

II. THE EUROPEAN UNION PRIVACY DIRECTIVES

In order to provide a firm understanding of the effect of the EU Directive, it is important to understand how the EU system works. The EU Commission, as the executive arm of the EU, proposes legislation and monitors how the legislation is implemented by the Member States.[5] Perhaps the most important role that the EU

---

[2] Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet,* 32 INT'L LAW. 991, 1001 (1998).

[3] *Id.*

[4] KUNER, *supra* note 1, at 20.

[5] *Id.* at 6.

Commission plays, in terms of data retention and protection, is determining when a non-EU state has implemented sufficient legislation to offer an "'adequate level' of data protection" before allowing data transference between two or more countries.[6] There are both substantive and procedural factors which must be met before an EU Member State will transfer data to another state. The substantive factors include the purpose for collecting the data, the quality and proportionality of the data, the transparency and security of the procedure, the rights of access to the data, and the restrictions on transferring the data to any other third parties.[7] The procedural factors include a high level of compliance with the rules, they require: a procedure for allowing individuals to exercise their privacy rights, and a procedure for allowing redress to individuals whenever the substantive rules are broken. The EU Commission can grant access to electronic data either wholesale, if the requesting state has implemented legislation that falls within the guidelines directly above, or on a case-by-case basis for certain projects.[8] Currently, the only States which have been approved to transfer data freely with EU Member States are Guernsey, Isle of Man, Switzerland, the U.S. (for corporations that have signed up and agreed to abide by the procedures/requirements of the Safe Harbor provisions), Canada, and Argentina.[9] Once a state's data protection legislation has been deemed adequate by the EU, no Member State can deny the transfer of personal information to that State. Moreover, if a violation of the data protection legislation occurs, it is the responsibility of the Member State, and not the EU, to prosecute or rectify the situation.[10]

The two primary pieces of EU legislation are the General Directive (Directive 95/46), which provides a framework for data protection, and the Directive on Privacy and Electronic Communications (Directive

---

[6] *Id.*

[7] *Id.* at 132-134.

[8] *Id.*

[9] *Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries, available at* http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm (last visited Jan. 17, 2006).

[10] DOROTHEE HEISENBERG, NEGOTIATING PRIVACY: THE EUROPEAN UNION, THE UNITED STATES, AND PERSONAL DATA PROTECTION 27-28 (2005).

2002/58), which provides more specific regulations.[11] The purpose of the EU General Directive is to "allow for the free flow of data within Europe" and to "achieve a harmonized minimum level of data protection throughout Europe."[12] The principles spelled out in the General Directive reflect these two purposes. These principles are:

- *Legitimacy*: personal data may only be processed for limited purposes;
- *Finality*: personal data may only be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes;
- *Transparency*: the data subject must be given information regarding data processing relating to him;
- *Proportionality*: personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed;
- *Confidentiality and security*: technical and organizational measures to ensure confidentiality and security must be taken with regard to the processing of personal data; and
- *Control*: supervision of processing by Data Protection Authorities ("DPAs") must be ensured.[13]

In order for a business or organization to be able to collect private information on individuals over the Internet, the above six principles must be somehow accounted for. In general, the EU Directive prohibits "listening, taping, storage or other kinds of interception or

---

[11] KUNER, *supra* note 1, at 23-24; Council Directive 95/46, 1995 O.J. (L. 281) (EC); Council Directive 2002/58 2002 O.J. (L. 201) (EC).

[12] *Id.* at 17.

[13] *Id.* at 17-18.

surveillance of communications. The communications service providers are obligated to delete all traffic data no longer required for the provision of a communications service."[14] However, there are some exceptions for national defense, security, criminal law,[15] and for "purely personal or household" uses.[16]

While the EU Commission is responsible for proposing legislation and monitoring the manner in which the Member States implement the legislation, ultimately the final word in enforcement lies with the Member States themselves. Member States are also responsible for developing national legislation and creating a national DPA[17] as part of their national legislation.[18] The legislation enacted by the individual Member States does not have to be completely uniform, but it does have to follow some standards. The laws have to meet the minimum standards of the Directive without being so intrusive so as to "impede data flows with other Member States (the maximum)."[19] Just as the national privacy legislation of the Member States can differ from each other, so too can the set-up of the DPA in each state. The DPA can either operate as a commission or with a single ombudsman.[20] The DPA's also act in an advisory role by giving advice to companies who are engaged in electronic commerce in their countries, though the companies are not obligated to consult with the DPA.[21]

With the establishment of both EU privacy laws and laws in each of the Member States, a common question is what law applies when a

---

[14] Abu Bakar Munir & Siti Hajar Mohd Yasin, *Retention of Communications Data: A Bumpy Road Ahead*, 22 J. MARSHALL J. COMPUTER & INFO. L. 731 (2004).

[15] KUNER, *supra* note 1, at 19.

[16] HEISENBERG, *supra* note 10, at 29.

[17] Article 28 of the General Directive requires that each Member State set up a national DPA (Data Protection Authority). Council Directive 95/46, art. 28, 1995 O.J. (L. 281) (EC). DPA's typically have enforcement duties under the federal data protection laws, but also may play an advisory role at the state and local level. KUNER, *supra* note 1, at 13-14.

[18] *Id.*

[19] *Id.* at 28-30.

[20] *Id.* at 14.

[21] *Id.* at 14-16.

conflict arises. The EU Commission is charged with monitoring the legislation of the Member States to ensure that they comply with the six principles of the EU Directive set forth above.[22] If the Commission finds that a Member State is in breach, a number of options can be implemented. First, the Commission can send the State a letter reminding them of their obligation.[23] A second option is to refer the case to the European Court of Justice ("ECJ"), which is the only organ that can legally interpret the data protection legislation.[24] The ECJ then has the ability to either "find the Member State in breach or impose a fine."[25]

The EU Directive created a safe environment for the transfer of data between member states. However, problems could arise regarding trade with states outside the EU systems if comparable legislation is not in place to protect any private information that might pass hands. This has led to the development of similar data protection laws in several states outside the EU system.[26]

III. RECENT DEVELOPMENTS REGARDING THE EU DIRECTIVE

A. LINDQVIST DECISION

One of the recent developments stemming from the EU Directives is that certain provisions are being considered by international courts such as the ECJ. The Lindqvist decision out of the ECJ is among the most important because it was the first decision that interpreted

---

[22] *Id.* at 6.

[23] KUNER, *supra* note 1, at 31.

[24] *Id.* at 7.

[25] *Id.* at 31.

[26] Swire, *supra* note 2, at 1002; additionally, a list of third countries the EU has determined have adequate levels of protection can be found at http://europa.eu.int/comm/justice_home/fsj/privacy/thridcountries/index_en.htm. Currently only Argentina, Canada, Switzerland, the U.S. (through the Passenger Name Record agreement and Safe Harbor provisions), Guernsey, and Isle of Man have been recognized as having adequate safeguards. Further information on the E.U. Directive can be found in CHRISTOPHER KUNER, EUROPEAN DATA PRIVACY LAW AND ONLINE BUSINESS (Oxford Univ. Press) (2003), and in PETER P. SWIRE AND ROBERT LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE (Brookings Institution Press) (1998).

Directive 95/46.[27] Mrs. Lindqvist, in her position as a catechist for her parish, set up a website from her home that was accessible through the parish's official website.[28] Lindqvist's website contained information about herself, her husband, and other parishioners including names, jobs, telephone numbers, and other personal information including the medical circumstances of one individual.[29] The information about the individuals on the website was obtained and posted without their consent.[30]

The website was promptly removed once Lindqvist learned of the discontent of the individuals whose personal information she had posted.[31] In addition to failing to consult the persons from the parish, Lindqvist also did not consult the Swedish supervisory authorities who are charged with the processing of personal data.[32] As a result, she was prosecuted under Swedish law for failing to provide the authorities with prior written notice, processing personal information (including medical information), and transferring this data to third countries without adequate data protection laws.[33]

Mrs. Lindqvist was convicted and fined, though she appealed the decision arguing that her actions did not violate the Directive.[34] The case came under consideration of the ECJ when the Swedish courts referred the following questions to the court.[35] First, does the listing of personal data fall under the provision of the Directive prohibiting "the processing of 'personal data wholly or partly by automatic means'?"[36]

---

[27] Flora J. Garcia, *Bodil Lindqvist: A Swedish Churchgoer's Violation of the European Union's Data Protection Directive Should Be a Warning to U.S. Legislators*, 15 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1205, 1219 (2005).

[28] Case C-101/01, In re Lindqvist, 2004 All E.R. 561.

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *In re Lindqvist*, 2004 All E.R. at 561.

[35] *Id.*

[36] *Id.* at 562.

If not, did the website violate "the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system within the meaning of Article 3(1)"[37] by making it possible to search the individuals by first name?[38] The Court determined that the information posted by Lindqvist did fall under the definition of "personal data" and that by posting the information on her home computer, she was in fact "processing" the personal data.[39]

As the answers to the above questions were yes, the following questions became relevant. First, were the actions of Lindqvist covered as one of the exceptions in Article 3(2)?[40] According to this provision, if the processing of personal information "falls outside the scope of Community law"[41] or "by a natural person in the course of a purely personal or household activity,"[42] then it falls outside the scope of the Directive.[43] Lindqvist sought to qualify her actions under the latter of these categories by arguing that when one processes information "free of charge and without any economic activity,"[44] the Directive does not control.[45] The Court found that although Lindqvist's actions did fall outside the scope of Community law, they were not purely personal or household activities because the information extended beyond an intimate group and was accessible to anyone through the church's website.[46] Moreover, the Court, when faced with the question of whether the posting of information, such as the name of an individual and the fact that she has an injured foot, fall

---

[37] *Id.* at 569.

[38] *Id.*

[39] *Id.* at 570.

[40] *In re Lindqvist*, 2004 All E.R. at 569.

[41] *Id.* at 571 (quoting European Council Directive 95/46, art. 3(1)).

[42] *Id.*

[43] *Id.*

[44] *Id.*

[45] *Id.*

[46] *In re Lindqvist*, 2004 All E.R. at 686.

under the health provision of Article 8(1), the Court answered in the affirmative.[47]

The next question set forth by the Swedish Court is whether the fact that information posted on a website in Sweden could be accessed by persons from a third country means that it "constitute(s) a transfer of data to a third country within the meaning of the Directive?"[48] A related question is whether the answer to the question directly above differs if no one from a third country actually accessed the Swedish website.[49] The Court found that the act of merely uploading data to a website that can be accessed by other persons cannot constitute a transfer of data.[50] Anything to the contrary would mean that Member States would have an obligation to prevent the loading of personal information because it could possibly be seen by person in third countries which do not have adequate data protection procedures in place.[51]

Finally, the Swedish Court set forth questions dealing with the scope of the Directive. First, do the restrictions of the Directive violate freedom of expression as set forth in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms?[52] The Court held that the Directive itself was not contrary to the right to freedom of expression and that the Member States' duty to implement legislation supports both data protection goals and freedom of expression.[53] Finally, can EU Member States implement greater privacy protection standards than those provided by the Directive?[54] The Court answered that so long as the provisions of the Member State are consistent with the Directive, there is nothing that

---

[47] *Id.* at 583. Article 8(1) states: "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life." Council Directive 95/46, art. 8, 1995 O.J. (L. 281) 1 (EC).

[48] *Id.* at 569.

[49] *Id.*

[50] *Id.* at 586.

[51] *Id.* at 586.

[52] *In re Lindqvist*, 2004 All E.R. at 569.

[53] *Id.* at 588.

[54] *Id.* at 569.

prevents that State from extending their legislation to areas outside the Directive.[55]

The implications of this decision could be far-reaching. It is now clear that the Directive is applicable to individuals and that it covers violations that affect even a small number of people.[56] Thus, within the EU system, individuals whose personal information is posted on a website without their consent now have a cause of action.[57]

B. BINDING CORPORATE RULES

One of the disadvantages of the EU Directive has been that some companies, which are located in third countries that have not made a contractual agreement with the EU to engage in multinational transfers, have been disadvantaged in the corporate market.[58] The Article 29 Working Party, as defined in the Directive, has attempted to address this problem by developing a list of corporate rules which, if agreed to, would bind the corporation and bring them into compliance with the minimum adequate safeguards required by the Directive.[59]

The checklist set forth by the Working Group establishes the guidelines to show what companies must do/show when they apply for approval.[60] Seven primary issues are addressed in the Working Document.

- Which data protection authority is the right one for your company to apply to?

---

[55] *Id.* at 705.

[56] Garcia, *supra* note 27, at 1230.

[57] *Id.*

[58] Eduardo Ustaran, *Binding Corporate Rules: The Answer to Global Processing?* INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (2006), *available at* https://www.privacyassociation.org/index.php?option=com_content&task=view&id=463&Itemid=125.

[59] *Id.*

[60] Article 29 Data Protection Working Party, *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules* (Apr. 14, 2005), *available at* http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf (more in depth information on each of these categories can be found at this cite).

- Information required for application.
- Evidence that the measures are internally and externally binding.
- Verification of compliance.
- Description of the processing and flows of information, including the purpose and scope of the information.
- Description of the data protection safeguards.
- Description of the reporting and recording system of the corporation.[61]

Although this piece of legislation sought to decrease inequalities among corporate competitors, there have been some criticisms of the Binding Corporate Rules ("BCR"). The most pressing of these concerns is that approval is determined on a case-by-case basis by the member states.[62] Just because a corporation has met the guidelines does not mean that they are automatically eligible to make data transfers with every Member State.[63] Moreover, because the national implementation of the Directive differs for each Member State it is not even clear as to whether the BCR would meet the minimum requirements in each State.[64] Although this system is less than perfect, it is a start for corporations who otherwise would be shut out of a growing market.

While the EU Directives have been the catalyst for most of the privacy legislation that has sprung up around the world,[65] there are

---

[61] *Id.*

[62] John Stephens, *ICRT Comments on Binding Corporate Rules* 2, INTERNATIONAL COMMUNICATIONS ROUNDTABLE (2003), *available at* http://www.icrt.org/pos_papers/2003/030930_EE.pdf.

[63] *Id.*

[64] *Id.*

[65] HEISENBERG, *supra* note 10, at 120.

other sources on which a state may base its privacy legislation. Following is a brief discussion of two such bodies of law: the European Council on Cybercrime and the OECD.

IV. THE EUROPEAN COUNCIL ON CYBERCRIME

The Cybercrime Convention ("Convention") as opposed to the EU Directives is focused primarily at preventing *crimes* that take place through or on the computer.[66] It was drafted and adopted into law in November 2001, by the Council of Europe, an organization that has forty-four member states.[67] Since its adoption by the Council of Europe, it has been signed by over thirty countries and ratified by eleven, and consequently entered into force in 2004.[68] In order to enter into force, the Convention needed to be ratified by five countries, three of which are members of the Council of Europe (which the above stated countries are). Now in force, the Convention acts as a multilateral treaty, binding the countries in a similar fashion.[69] The Convention is the first international treaty that addresses crimes that take place on and through computer systems.[70]

The goal of the Convention is to establish a minimum set of guidelines that states can integrate into their domestic laws.[71] The purpose of making these regulations so general is to permit them to fit into the domestic legal systems of each participating state.[72] This is

---

[66] U.S. Department of Justice (USDOJ), *Council of Europe Convention on Cybercrime, Frequently Asked Questions and Answers*, http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm (last visited Nov. 27, 2005).

[67] *Id.*

[68] Global Internet Policy Initiative, *Trust and Security in Cyberspace: The Legal and Policy Framework for Addressing Cybercrime* 4, (2005), *available at* http://www.internetpolicy.net/cybercrime/20050900cybercrime.pdf.

[69] *Id.*; Mike Keyser, *Article: The Council of Europe Convention on Cybercrime*, 12 J. TRANSNAT'L L. & POL'Y 287, 296 (2003).

[70] Yamin Akdeniz, *An Advocacy Handbook for the Non Governmental Organisations* 3 (2005), *available at* http://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf.

[71] USDOJ, *supra* note 66.

[72] *Id.*

particularly difficult given the increased privacy protections given to individuals in European states and the heightened personal rights guaranteed by the Bill of Rights in the U.S.[73] The primary reasons for establishing an international set of guidelines for dealing with cybercrime are

> (1) the absence of a global consensus on the types of conduct that constitute a cybercrime; (2) the absence of a global consensus on the legal definition of criminal conduct; (3) the lack of expertise on the part of police, prosecutors and courts in the field; (4) the inadequacy of legal powers for investigation and access to computer systems, including the inapplicability of seizure powers to computerized data; (5) the lack of uniformity between the different national procedural laws concerning the investigation of cybercrimes; (6) the transnational character of many cybercrimes; and (7) the lack of extradition and mutual legal assistance treaties, synchronized law enforcement mechanisms that would permit international cooperation in cybercrime investigations, and existing treaties that take into account the dynamics and special requirements of these investigations.[74]

The offenses were based upon recommendations from both private and public organizations.[75] They deal with nine different offenses including: "illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography and offenses related to copyright."[76] The objective is to "pursue . . . a common criminal policy aimed at the protection of society against cybercrime. . . especially by adopting appropriate legislation and

---

[73] Shannon L. Hopkins, *Cybercrime Convention: A Positive Beginning to a Long Road Ahead*, 2 J. HIGH TECH. L. 101 (2003).

[74] Miriam F. Miquelon-Weismann, *The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process?* 23 J. MARSHALL J. COMPUTER & INFO. L. 329, 335 (2005).

[75] Keyser, *supra* note 69, at 299.

[76] Miquelon-Weismann, *supra* note 74, at 336.

fostering international co-operation."[77] Among the provisions of the Convention are regulations on the minimum laws which must be adopted by the participating states, the procedural and prosecutorial laws that must accompany them, the rules on how states are to participate in international investigations, and the specifics of applying the Convention.[78]

Each year there are more than $15 billion globally in damages as a result of cyber crime,[79] the majority of which are perpetrated by employees.[80] A perpetrator in the U.S. can commit a crime that can affect persons throughout the world. It is for this reason that jurisdiction to prosecute cyber crimes is such a problem. The Convention addresses these issues by requiring states to take jurisdiction over any cyber crimes that are: "committed within its territory, on board a ship flying that state's flag, on board an aircraft registered under the laws of that state or by one of its nationals if punishable by criminal law where committed."[81] However, situations can, and have arisen where jurisdiction is questionable. This is an issue that has not been sufficiently dealt with by the Convention.

While the U.S., overall, appears to be supportive of the Convention (President Bush submitted the Convention to the Senate for its advice and consent in November 2003),[82] there have been some major critiques of the Convention including concerns by the Electronic Privacy Information Center ("EPIC"), a public interest research center, and the Center for Democracy and Technology ("CDT").[83] In a statement to the Committee on Foreign Relations, EPIC expressed concerns about the possible civil liberty violations threatened by the Convention.[84] An example of the possible violations includes an

---

[77] Keyser, *supra* note 69, at 297.

[78] *Id.*

[79] Hopkins, *supra* note 73, at 108.

[80] *Id.* at 109.

[81] *Id.* at 118.

[82] USDOJ, *supra* note 66.

[83] Critiques from EPIC can be found at http://www.epic.org; Critiques from the CDT can be found at http://www.cdt.org.

[84] Letter from Marc Rotenberg, EPIC President & Cedric Laurant, EPIC Director, International Privacy Project, Policy Counsel to Sen. Richard G. Lugar, U.S. Senate Foreign

invasion of privacy through investigatory measures taken without the protection of judicial review.[85] Moreover, the privacy safeguards that are provided for in the Convention are too vague and weak to be in any way meaningful.[86] A concern, focused on law enforcement, is that the Convention does not require the violative action to be a crime in both jurisdictions.[87] So long as an action is a crime in one country, any others involved are required to aid in the investigation and prosecution even if the action is legal in their territory.[88] The final concern of EPIC is that the Convention has not been widely ratified, thus pointing to the hesitancy of many countries to hold themselves responsible for carrying out the obligations of the Convention.[89]

The CDT's apprehensions also focus on civil liberty issues. Among their concerns, the organization urges the Council of Europe to reject provisions that will "require Internet Service Providers to retain records regarding the activities of their customers"[90] because they are at odds with provisions of the European Directive.[91] Moreover, the CDT is concerned with the criminal consequences for engaging in copyright infringement, particularly since it is an area in which there has not been a clear principle of international law developed.[92] Finally, the CDT shares some of the same law enforcement concerns as EPIC. In particular, they are concerned that there is no uniform

---

Relations Committee Chairman & Sen. Joseph R. Biden, J.R., U.S. Senate Foreign Relations Committee Ranking Member (July 26, 2005), *available at* http://www.epic.org/privacy/intl/senateletter-072605.pdf [hereinafter EPIC Criticism].

[85] *Id.* at 1.

[86] *Id.* at 2.

[87] *Id.* at 3-4.

[88] *Id.*

[89] *Id.* at 4-5.

[90] Center for Democracy & Technology, *International Issues: Cybercrime*, (Oct. 18, 2000), *available at* http://www.cdt.org/international/cybercrime/001018cdt.shtml (last visited Feb. 12, 2006).

[91] *Id.*

[92] *Id.*

procedure for investigations.[93] It is yet to be seen whether these concerns will come to fruition.

V. THE ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The Organisation for Economic Co-operation and Development ("OECD") came into force on September 30, 1961.[94] There are thirty states that are parties to the OECD.[95] The organization adopted The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980 (Privacy Guidelines), thus becoming the first intergovernmental organization to issue guidelines in the privacy arena.[96] These principles are meant to reflect the three main goals of the OECD including: "pluralistic democracy, respect for human rights and open market economies."[97]

The OECD is divided into five sections:

- The first sets forth definitions of data controllers, personal data, and transborder flows of personal data, as well as setting forth the scope of the guidelines.[98]

---

[93] *Id.*

[94] Article 14 specifies when this Convention goes into effect. *See* OECD, *Organisation for the Economic Co-operation and Development,* http://www.oecd.org/document/7/0,2340,en_2649_201185_1915847_1_1_1_1,00.html (last visited Aug. 6, 2006); OECD, *Ratification of the Convention on the OECD,* http://www.oecd.org/document/1/0,2340,en_2649_201185_1889402_1_1_1_1,00.html (last visited Aug.6, 2006).

[95] *Id.* (Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States).

[96] OECD, *Protection of Privacy and Personal Data,* http://www.oecd.org/document/26/0,2340,en_2649_34255_1814170_1_1_1_1,00.html. (last visited Nov. 27, 2005).

[97] OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT 7, (2002) [hereinafter OECD].

[98] *Id.* at 13-14.

- The second section sets forth the seven principles of the guidelines. The principles are a limitation of the collection of personal data, the data quality principle, the requirement that the purposes for personal data should be specified, a limitation on the disclosure of personal data, the protection through use of reasonable safeguards, a policy of openness, a requirement giving rights to individuals regarding the use of their data, and insuring that controllers are accountable for compliance with the principles laid out above.[99]

- The third section deals with how states will deal with transborder flows of information.[100]

- The fourth section deals with how member states are to comply on a national level.[101]

- Finally, section five addresses how states are to share information and investigatory powers with each other.[102]

The objectives of the OECD Guidelines are to achieve a minimum standard of privacy protection among the parties, to reduce the differences between the domestic laws, to avoid interfering with the free flow of information, and finally to reduce the restrictions on international information transfers due to individual privacy risks these restrictions might cause.[103] However, as with most other data protection legislation, questions remain as to whom the rules should apply and under what circumstances. For instance, do the protections apply equally to corporations as they do to individuals? Should certain

---

[99] *Id.* at 14-16.

[100] *Id.* at 16-17.

[101] *Id.* at 17.

[102] *Id.* at 18.

[103] OECD, *supra* note 97, at 32.

groups, such as persons with disabilities or minors, receive greater protection?[104] These are questions which have not yet been answered, but the OECD, along with other governmental and non-governmental organizations are addressing these concerns. The OECD has issued subsequent guidelines, including the 1985 Declaration on Transborder Data Flows and the Ministerial Declaration on the Protection of Privacy on Global Networks.[105]

The above discussions of the EU Directive, the Cybercrime Convention, and the OECD Guidelines represent the growing field of privacy legislation addressing the transborder flows of information. Some are primarily focused on preventing cyber crimes, while others focus on protecting individual's rights during the transfer of electronic data. However, each of them is focused on the regulation of information via the computer. These actions, even though they can affect multiple persons in multiple locations, usually fall under the jurisdiction of one state. The following are examples of how two domestic legal systems have dealt with electronic privacy issues. First, a discussion of the legislation coming out of the United Kingdom – a member of the EU, and second, a discussion of legislation from the U.S.

VI. UK LEGISLATION

After the terrorist events of September 11, 2001, the world became much more concerned with protecting itself against terrorist attacks. The United Kingdom is no different in its desire to retain electronic data for the purposes of national security. Among the legislation passed by the UK are the Identity Cards Bill (2005), the Regulation of Investigatory Powers Act of 2000 and the Anti-Terrorism Crime and Security Bill Act of 2001.

A. IDENTITY CARDS BILL (2005)

In response to the recent terrorist attacks in London and around the world, several governments have considered establishing a national identification card system. The UK has joined these countries and introduced the Identity Cards Bill which, if passed, is expected to be in

---

[104] *Id.* at 34.

[105] *Id.*

effect by 2010.[106] The ID cards will include biometric features, including facial images, iris patterns, and fingerprints.[107] The rationale behind these new precautions is protection against identity theft, illegal immigration and working, misuse of public services, and perhaps most importantly, organized crime and terrorism.[108] The government claims that the ID cards will be a more secure form of identification because the personal details of each individual will be checked upon their application, recording procedures will keep individuals from assuming multiple identities, and it will be harder to forge identity documents since the new ID's will be checked electronically.[109]

The Identity Cards Bill is justified partly on the basis that the EU has begun: (1) requiring biometric passports for citizens of EU Member States traveling to the Schengen region, and (2) supporting biometric passports for foreign nationals seeking residency permits or work visas within the EU.[110] However, these biometric identification cards have been the focus of much debate, both within the UK and around the world. At the top of the list of problems with the new identity cards is the cost.[111] Costs for the British system is estimated at approximately $5.6 billion.[112] It appears that the current plan is for the ID cards to be voluntary, however, some ministers are concerned that this initial scheme will only pave the way for a future system in which the cards, and thus registration in the national register, are required in order to obtain documents such as a passport or driver's license.[113]

---

[106] Laura Rohde, *U.K. Biometric ID Cards Bill Shelved Before Election: Labor Party blames Conservatives for killing legislation*, COMPUTER WORLD (Apr. 6, 2005) *available at* http://www.computerworld.com/securitytopics/security/story/0,10801,100891,00.html (last visited Jan. 16, 2006).

[107] Home Office, *Identity Cards Briefing* 4, (May 2005), *available at* http://www.identitycards.gov.uk/downloads/Id_Cards_Briefing.pdf.

[108] *Id.* at 1-3.

[109] *Id.*

[110] *Id.*

[111] Rohde, *supra* note 106.

[112] *Id.*

[113] George Jones, *Tories Ambush Blair on Identity Cards* TELEGRAPH.CO.UK (Dec. 27, 2005) *available at* http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2005/12/27/nid27.xml&sSheet=/news/2005/12/27/ixnewstop.html (last visited Jan. 16, 2006).

B. REGULATION OF INVESTIGATORY POWERS ACT AND THE UK ANTI-TERRORISM CRIME AND SECURITY BILL

The Regulation of Investigatory Powers ("RIP") Act of 2000 and the Anti-Terrorism Crime and Security Bill ("ATCSB") (2001) allow the government to track and analyze the patterns of citizens through traffic analysis, blanket data retention, and mass-surveillance.[114] These acts allow the government to more easily intercept phone and e-mail information by forcing phone companies and internet providers to "install interception devices in their network."[115] The primary purpose of the Act is to enhance the state's security capabilities by forcing the retention of data for certain periods of time.[116] However, there are a number of secondary goals surrounding the implementation of this legislation including: cutting off funding for terrorists, giving the government the necessary tools for collecting information to fight terrorism, streamlining immigration procedures, stopping religious and racial hatred, safeguarding nuclear and aviation industries, increasing the protection against chemical or biological weapons, increasing police power, and complying with the obligations of the EU and updating the state's anti-terrorist measures.[117]

The secondary goals stated above make up the fourteen parts of the ATCSB. The twelve main principles are as follows:

- Part One: allows the government to investigate and freeze any funds that could be used to finance terrorist activities.

- Part Two: gives the government the ability to freeze the assets of governments or residents overseas.

---

[114] Casper Bowden, *Closed Circuit Television for Inside your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation*, 5 DUKE L. & TECH. REV. 1-2 (2002).

[115] Ian Brown, *Communications Surveillance Briefing*, FIPR: FOUNDATION FOR INFORMATION POLICY RESEARCH (Aug. 18, 2003), http://www.fipr.org/030818ripa.html (last visited Nov. 27, 2005).

[116] *Id.*

[117] Anti-Terrorism, Crime, and Security Bill, 2001, H.C. Bill [49], (Gr. Brit.), *available at* http://www.publications.parliament.uk/pa/cm200102/cmbills/049/en/02049x--.htm (last visited Nov. 27, 2005).

- Part Three: allows the customs agency to share information with law enforcement agencies.
- Part Four: allows for the government to detain suspected terrorists, to speed up the asylum process, and to remove judicial review of these actions.
- Part Five: makes religiously motivated crimes equal to racially motivated crimes.
- Part Six: strengthens legislation regarding weapons of mass destruction.
- Part Seven: increases the safeguards on chemical and biological weapons.
- Part Eight: increases the inspection and regulation of nuclear sites.
- Part Nine: increases restrictions in airports and aircrafts to guard against terrorist activities.
- Part Ten: expands the police power of customs agents, transport police, and ministry of defense police.
- Part Eleven: re-affirms the authority of communications service providers to retain data.
- Part Twelve: gives the courts jurisdiction over crimes of bribery committed by foreign public officials, Ministers, MPs and judges.[118]

In addition to collecting and retaining data for security reasons, these acts allow the government to access data for "public order, minor crime, health and safety and tax."[119] Though companies are not

[118] *Id.*

[119] Bowden, *supra* note 114, at 8.

obligated to record any data, once the government has lawfully obtained it under this legislation, it can be retained for up to three years.[120]

VII. UNITED STATES LEGISLATION

While the approach of the EU to data protection is omnibus, targeting public and private sectors, the U.S. approach is more sectoral, usually addressing only the public sector.[121] The U.S. has implemented two distinct pieces of legislation, each seeking to regulate data protection in a separate manner.[122] The first is the Safe-Harbor Provision which is focused primarily on economic provisions.[123] The second is the Passenger Name Record which focuses more on national security purposes.[124]

A. THE SAFE-HARBOR PRIVACY PROVISION

The economic relationship between the EU and the U.S. made creating a procedure for complying with the EU Directive a necessity for the U.S. Over forty percent of U.S. investments abroad are located in EU Member States and almost twenty percent of U.S. exports go to the EU.[125] Therefore the U.S. adopted the Safe-Harbor Privacy provision on November 1, 2000.[126] The provision was deemed by the EU Commission to be an adequate protection for electronic transfers

---

[120] *Id.* at 10, 13.

[121] Steven Bellman et al., *International Differences in Information Privacy Concerns: A Global Survey of Consumers*, 20 THE INFO. SOC'Y 313, 315 (2004).

[122] Europa, *Commission Decisions on the Adequacy of Protection of Personal Data in Third Countries, available at* http://ec.europa.eu/comm/external_relations/us/intro/pnrmem03_53.htm (last visited Sept. 27, 2006); http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

[123] U.S. Department of Commerce, Introduction to the Safe Harbor, http://www.export.gov/safeharbor/index.html (last visited Sept. 27, 2006).

[124] HEISENBERG, *supra* note 10, at 140-142.

[125] PATRICK R. HUGG, A GUIDE TO EUROPEAN UNION COMMERCIAL PRACTICE 3 (Oceana Publications, Inc) (2003).

[126] HEISENBERG, *supra* note 10, at 74-75.

thus allowing any company that signs the Safe Harbor Agreement to freely transfer data to and from EU Member States.[127] There are seven fair information principles that make up the Safe Harbor provisions. They are:

- Notice: They will notify customers how they will use their personal data, and before they transfer it to another organization, or it is used for a purpose other than that for which it was collected.

- Choice: They will allow customers to opt out before sending their data to a third party or use it for a different purpose.

- Onward Transfer: They may only transfer data to another company (after giving notice and choice) if that company is in Safe Harbor, or has some other adequacy finding.

- Security: They must take reasonable precautions to protect the data from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

- Data Integrity: They should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

- Access: They must ensure that individuals have access to the information that the companies have about them, and be able to correct, amend, or delete information that is inaccurate, except in cases where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy, or where the rights of persons other than the individual would be violated.

---

[127] *Id.*

- Enforcement: They must provide readily available and affordable independent recourse for individuals who believe their privacy has been violated, investigation of each individual's complaints and disputes, and award damages where appropriate.[128]

A U.S. organization or company can send or receive electronic data between itself and EU Member States by self-certifying annually with the Department of Commerce, making a public declaration, and agreeing to adhere to the safe harbor provisions.[129] Once an organization or corporation agrees to adhere to the principles of the Safe Harbor provision, they must subject themselves to both self-enforcement and governmental enforcement. In terms of self-enforcement, each organization must implement a dispute resolution system, which will investigate individual complaints and develop remedies for any compliance problems that arise.[130] Self-regulation, however cannot be the only means of enforcement. Therefore, the government, either through the Federal Trade Commission or another regulatory agency, should step in when a company or organization fails to comply with the self-regulatory principles. The punishment for failing to comply with the Safe Harbor regulations includes monetary damages or revocation of Safe Harbor benefits.[131]

B. PASSENGER NAME RECORD

The Passenger Name Record ("PNR") is a provision of the Aviation and Transportation Security Act which was passed by Congress in November 2001.[132] The Act requires airlines to gather

---

[128] *Id.*

[129] U.S. Department of Commerce, Safe Harbor Overview, http://www.export.gov/safeharbor/sh_overview.html (last visited Nov. 27, 2005).

[130] *Id.*

[131] *Id.* Forms and further information on the certification process a corporation must follow to be covered under the Safe Harbor Provision can be found at the U.S. Department of Commerce's website: http://www.export.gov/safeharbor/sh_overview.html.

[132] Europa, *Airline Passenger Data Transfers from the EU to the United States (Passenger Name Record), available at* http://ec.europa.eu/comm/external_relations/us/intro/pnrmem03_53.htm (last visited Aug. 2006).

passenger data on all commercial flights passing through the U.S. This information includes: name, age, country of origin, height and weight, race, where passenger would stay upon arrival, visa information, and information from the purchase of the flight such as email, credit card details, telephone numbers, dietary preferences and other general remarks.[133] This information would then be entered into a computer system that would screen for potential terrorists.[134] This information has been provided to the U.S. Customs and Border Protections (USCBP) in an effort to guard against terrorism.[135] However, due to the nature and means of the information collected, there has been conflict with the EU Directive.[136] The Department of Homeland Security (DHS) and the EU Commission have struggled to come to an agreement which would allow the U.S. to maintain its system of collecting passenger data while still falling under the guidelines of the EU privacy laws. Without an agreement, airlines would be subject to fines from EU States.[137]

An agreement between DHS and the EU Commission was reached in December 2003 which allowed airlines to share information with the USCBP regarding flights that originated in EU countries.[138] This provisional agreement was based largely on the safeguards of the USCBP system.[139] The EU Commission finally adopted an adequacy finding in February 2004 which gives the USCBP access to PNR data originating from Europe, though with certain limitations.[140] Despite disagreement from the European Parliament, the EU Commission announced the adequacy finding on May 17, 2004, and it was

---

[133] HEISENBERG, *supra* note 10, at 140-142.

[134] *Id.*

[135] Press Release, Department of Homeland Security, Fact Sheet: US-EU Passenger Name Record Agreement Signed (May 28, 2005), *available at* http://www.dhs.gov/dhspublic/display?content=3651 (last visited Nov. 27, 2005) [hereinafter Press Relase DHS].

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Id.*

approved by the Council.[141] In November 2005, the Advocate General of the ECJ recommended the annulment of the agreement reached between the EU and U.S. regarding the transfer of passenger data.[142] Though not binding on the Court, the Attorney General proposed that the Court reverse not only the adequacy decision but also the Council's decision.[143] It appears that the adequacy finding will be challenged in the ECJ some time during 2006.

VIII. CONCLUSION

Data protection has become a hot topic within the international community. Several legislative bodies have sought to deal with this topic – some for the protection of individual privacy rights, some for the protection of the government against terrorist acts. With the tensions between these two goals, many states are torn between the two, usually opting for legislation that addresses both concerns. The UK and U.S. are two such examples. The UK, as a member of the EU, has passed legislation protecting the rights of individuals in the transborder transfer of data, but it has also passed the Identity Cards Bill, the RIP Act, and the ATCSB, which focus on reducing terrorist threats against the State. The U.S., in an effort to protect its economic relationship with the EU has passed the Safe Harbor Provisions, which provide adequate protections for the transfer of data. However, the Bush Administration, in an effort to control terrorism in the U.S., implemented the PNR Provision, which threatened to stall airplane travel between the U.S. and EU because of discrepancies in data protection regulations.

The international bodies of law regarding data protection all strive to create some degree of uniformity among the international community. Despite the challenges of varying legal systems and

---

[141] Press Relase DHS, *supra* note 135.

[142] Digital Civil Rights in Europe, *Advocate General European Court Rejects PNR Deal* (Dec. 5, 2005) *available at* http://www.edri.org/issues/privacy/pnr (last visited Jan. 17, 2006).

[143] Press Release, Court of Justice of the European Communities, Advocate General Leger Proposes Annulment of the Commission and Council Decisions on Transfer to the American Authorities of Personal Information Concerning Air Passengers (Nov. 22, 2005) *available at* http://curia.eu.int/en/actu/communiques/cp05/aff/cp050098en.pdf (last visited Jan. 17, 2006); The full text of the Attorney General's opinion can be found at http://curia.eu.int/en/actu/communiques/cp05/aff/cp050098en.pdf.

moral emphasis, it appear that these bodies of legislation will increasingly gain adherence due to the increased global commerce involving the transfer of electronic data as well as the increased concerns of terrorism. For now, the EU Directive, Cybercrime Convention, and the OECD Guidelines provide a good foundation on which individual states can base their own data protection legislation.